IPv6 Network Reconnaissance:
Theory & Practice

Fernando Gont

SI6 NETWORKS

IEPG 86
Orlando, Florida, U.S.A. March 10, 2013

Overview

- IPv6 changes the “Network Reconnaissance” game
- Brute force address scanning attacks undesirable (if at all possible)
- Security guys will need to evolve in how they do net reconnaissance
  - Pentests/audits
  - Deliberate attacks

IPv6 Network Reconnaissance

- Address scans
- DNS-based (AXFR, reverse mappings, etc.)
- Application-based
- Inspection of local data structures (NC, routing table, etc.)
- Inspection of system configuration and log files
- “Snooping” routing protocols
- draft-ietf-opsec-ipv6-host-scanning is your friend :-)

IPv6 Address Scanning
Local Networks

SI6 NETWORKS

Overview

- Leverage IPv6 all-nodes link-local multicast address
- Employ multiple probe types:
  - Normal multicasted ICMPv6 echo requests (don't work for Windows)
  - Unrecognized options of type 10xxxxxx
- Combine learned IIDs with known prefixes to learn all addresses
- Technique implemented in the scan6 tool of SI6's IPv6 toolkit

Possible mitigations

- Do not respond to multicasted ICMPv6 echo requests
  - Currently implemented in Windows
- Multicasted IPv6 packets containing unsupported options of type 10xxxxxx should not elicit ICMPv6 errors
  - See draft-gont-6man-ipv6-smurf-amplifier
- **However**, it's virtually impossible to mitigate IPv6 address scanning of local networks
  - Think about mDNS, etc.

IPv6 Address Scanning
Remote Networks

SI6 NETWORKS

Overview

- IPv6 address-scanning attacks have long been considered unfeasible
- This myth has been based on the assumption that:
  - IPv6 subnets are /64s, **and**,
  - Host addresses are “randomly” selected from that /64

IPv6 addresses in the real world

- Malone measured (*) the address generation policy of hosts and routers in real networks

Address type	Percentage
SLAAC	50%
IPv4-based	20%
Teredo	10%
Low-byte	8%
Privacy	6%
Wordy	<1%
Others	<1%

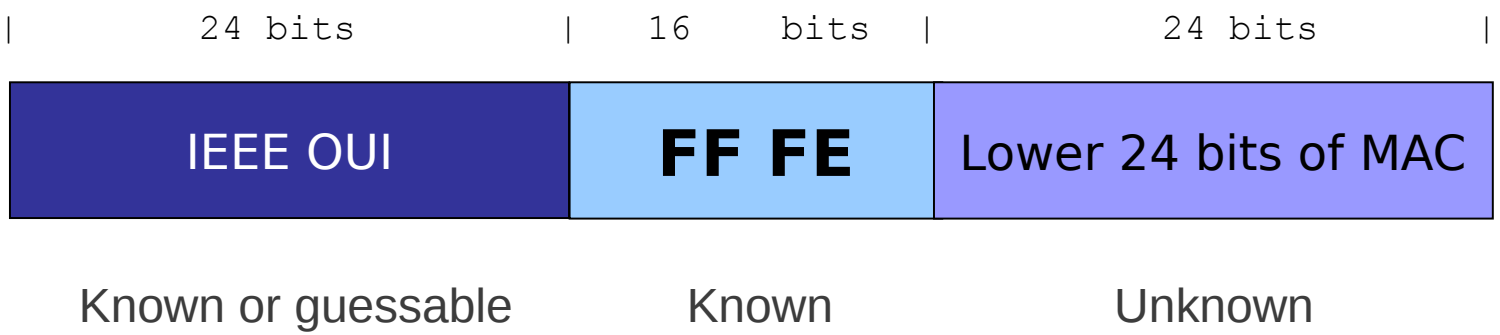
Hosts

Address type	Percentage
Low-byte	70%
IPv4-based	5%
SLAAC	1%
Wordy	<1%
Privacy	<1%
Teredo	<1%
Others	<1%

Routers

Malone, D., "Observations of IPv6 Addresses", Passive and Active Measurement Conference (PAM 2008, LNCS 4979), April 2008, <http://www.maths.tcd.ie/~dwmalone/p/addr-pam08.pdf>.

IPv6 addresses embedding IEEE IDs



- In practice, the search space is at most ~2^{23} bits – **feasible!**
- The low-order 24-bits are not necessarily random:
  - An organization buys a large number of boxes
  - In that case, MAC addresses are usually consecutive
  - Consecutive MAC addresses are generally in use in geographically-close locations

IPv6 addresses embedding IEEE IDs (II)

- Virtualization technologies present an interesting case
- Virtual Box employs OUI 08:00:27 (search space: ~2^{23})
- VMWare ESX employs:
  - Automatic MACs: OUI 00:05:59, and next 16 bits copied from the low order 16 bits of the host's IPv4 address (search space: ~2^{8})
  - Manually-configured MACs:OUI 00:50:56 and the rest in the range 0x000000-0x3fffff (search space: ~2^{22})

IPv6 addresses embedding IPv4 addr.

- They simply embed an IPv4 address in the IID
  - e.g.: 2000:db8::192.168.0.1
- Search space: same as the IPv4 search space – feasible!

IPv6 addresses embedding service ports

- They simply embed the service port the IID
  - e.g.: 2001:db8::80
- Search space: smaller than 2^8 – feasible!

IPv6 “low-byte” addresses

- The IID is set to all-zeros, except for the last byte
  - e.g.: 2000:db8::1
  - There are other variants..
- Search space: usually 2^8 or 2^{16} – feasible!

IPv6 Address Scanning
Practice

SI6 NETWORKS

scan6 tool

- Address scanning of the SI6 IPv6 toolkit
- Available for Linux, *BSD, and Mac OS X
- Supports Ethernet and tunnels
- Free software
- Available at: http://www.si6networks.com/tools/ipv6toolkit

Practice

- Local scans:

  # scan6 -i eth0 -l -v

- Remote “brute force” scan:

  # scan6 -i eth0 -v -d fc00:1::/64

  # scan6 -i eth0 -v -d fc00:1::0-ffff:0-ffff:0-100:0-100

- Targetting virtual machines:

  # scan6 -i eth0 -v -d fc00:1::/64 --tgt-virtual-machines all

  # scan6 -i eth0 -v -d fc00:1::/64 --tgt-virtual-machines vbox

Practice (III)

- Target a known IIDs (added yesterday :-)):

  # scan6 -i eth0 -d fc00:1::/64 -v --tgt-known-iids FILE

Thanks!

Fernando Gont

fgont@si6networks.com

www.si6networks.com